

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-readable medium included in a storage device and having embodied thereon a computer program configured to determine whether a user is permitted to access requested attributes of a business object when executing a software application of an enterprise information technology system, the medium storing one or more code segments configured to:

use a permission object to determine whether a user associated with an entry in user information is permitted to access requested attributes ~~at least part~~ of a data object associated with a data object type, wherein:

the entry in the user information associates the user with a user affiliation,

the permission object identifies:

a user affiliation to which the permission object applies,

a data object type to which the permission object applies such that the data object type identified by the permission object is associated with multiple attributes and each data object having the data object type identified by the permission object is associated with the multiple attributes,

a permission attribute identifying at least one of the multiple attributes,

a permission value for the permission attribute, and

an attribute access group having a subset of one or more attributes of the multiple attributes ~~associated with the data object type identified by the permission object, the~~ subset of attributes being fewer than all of the multiple attributes, wherein the permission

object is configured to use the permission attribute included in the attribute access group and to use the permission attribute not included in the attribute access group,

wherein upon determination that:

(1) the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the permission object applies,

(2) the data object type of the data object is the same as the data object type to which the permission object applies,

(3) a value of the permission attribute ~~an attribute of the multiple attributes~~ associated with the data object is consistent with the permission value for[[of]] the permission attribute ~~and the attribute corresponds to the permission attribute~~, and

(4) at least one of the requested attributes of the data object ~~at least one attribute of the data object that the user seeks to access~~ corresponds to an attribute of the attribute access group of the permission object,

the user is permitted to access any of the requested attributes indicated by the attribute access group ~~and not permitted to access any of the requested attributes not associated with the attribute access group~~ ~~the attribute sought to be accessed~~, and wherein otherwise the user is denied access to all the requested attributes ~~sought to be accessed~~.

2. (Previously Presented) The medium of claim 1 wherein the one or more code segments are further configured to permit the user to access at least part of the data object when the value of the attribute of the multiple attributes associated with the data object is the same as the permission value of the permission attribute.

3. (Previously Presented) The medium of claim 1 wherein the one or more code segments are further configured to permit the user to access at least part of the data object when the value of the attribute of the multiple attributes associated with the data object is within a range specified by the permission value of the permission attribute.

4. (Previously Presented) The medium of claim 1 wherein the one or more code segments are further configured to permit the user to access at least part of the data object when the value of the attribute of the multiple attributes associated with the data object is one of enumerated values specified by the permission value of the permission attribute.

5-6. (Canceled)

7. (Previously Presented) The medium of claim 1 wherein:
the permission object identifies a permitted action, and
the one or more code segments are further configured to permit the user to access at least part of the data object and perform an action on the data object when the action is consistent with the permitted action identified in the permission object.

8. (Currently Amended) A method for determining whether a user is permitted to access requested attributes of a business object when executing a software application of an enterprise information technology system, the method comprising:

using a permission object included in a storage object to determine whether a user associated with an entry in user information is permitted to access requested attributes at least part of a data object associated with a data object type, wherein:

the entry in the user information associates the user with a user affiliation,
the permission object identifies:

a user affiliation to which the permission object applies,
a data object type to which the permission object applies such that the data object type identified by the permission object is associated with multiple attributes and each data object having the data object type identified by the permission object is associated with the multiple attributes,

a permission attribute identifying at least one of the multiple attributes,
a permission value for the permission attribute, and

an attribute access group having a subset of one or more attributes of the multiple attributes ~~associated with the data object type identified by the permission object,~~
the subset of attributes being fewer than all of the multiple attributes, wherein the permission object is configured to use the permission attribute included in the attribute access group and to use the permission attribute not included in the attribute access group,
wherein upon determination by a processor that

(1) the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the permission object applies,

(2) the data object type of the data object is the same as the data object type to which the permission object applies,

(3) a value of the permission attribute ~~an attribute of the multiple attributes~~ associated with the data object is consistent with the permission value for~~for~~ the permission attribute ~~and the attribute corresponds to the permission attribute,~~ and

(4) at least one of the requested attributes of the data object ~~at least one attribute of the data object that the user seeks to access~~ corresponds to an attribute of the attribute access group of the permission object,

the user is permitted using the processor to access any of the requested attributes indicated by the attribute access group ~~the attribute sought to be accessed,~~ and wherein otherwise the user is denied access to all the requested attributes ~~sought to be accessed.~~

9. (Previously Presented) The method of claim 8 further comprising permitting the user to access at least part of the data object when the value of the attribute of the multiple attributes associated with the data object is the same as the permission value of the permission attribute.

10. (Previously Presented) The method of claim 8 further comprising permitting the user to access at least part of the data object when the value of the attribute of the multiple attributes associated with the data object is within a range specified by the permission value of the permission attribute.

11. (Previously Presented) The method of claim 8 further comprising permitting the user to access at least part of the data object when the value of the attribute of the multiple attributes associated with the data object is one of enumerated values specified by the permission value of the permission attribute.

12. (Canceled)

13. (Currently Amended) A computer system for determining whether a user is permitted to access requested attributes ~~at least part~~ of a data object when executing a software application of an enterprise information technology system, the system tangibly embodied and comprising:

a processor;

a storage device including a data repository for access control information for software having data objects, each data object

(1) being associated with a data object type having multiple attributes,

(2) having the multiple attributes of the data object type to which the data object is associated, and

(3) having a value associated with each attribute of the multiple attributes, the data repository including:

user information that associates a user affiliation with a user of the software application, and

permission information having multiple permission objects, each permission object identifying a user affiliation to which the permission object applies, a data object type to which the permission object applies, a permission attribute identifying one of the multiple attributes, a permission value for the permission attribute, and an attribute access group having a subset of one or more attributes of the multiple attributes, the subset of attributes being fewer than all of the multiple attributes, wherein the permission object is configured to use the permission attribute included in the attribute

access group and to use the permission attribute not included in the attribute access group of the data object type; and

an executable software module executed by the processor that causes:

a comparison of a value of a[n] requested attribute of the multiple attributes of a data object ~~to which a user seeks access~~ such that the attribute of the multiple attributes corresponds to the permission attribute of a permission object with the permission value of the permission object,

a comparison of at least one attribute of the data object that the user seeks to access such that the attribute sought to be accessed corresponds to an attribute of the attribute access group of the permission object, and

an indication that a user is permitted to access any of the requested attributes indicated by the attribute access group and not permitted to access any of the requested attributes not associated with the attribute access group ~~the attribute sought to be accessed~~ when

(1) the value of the attribute of the data object is consistent with the permission value of the permission object, and

(2) at least one of the requested attributes of the data object ~~attribute of the data object that the user seeks to access~~ corresponds to an attribute of the attribute access group of the permission object, and

wherein otherwise the user is denied access to all the requested attributes ~~sought to be accessed~~.

14. (Previously Presented) The system of claim 13 wherein the executable software module causes an indication that a user is permitted to access the attribute sought to be accessed when the value of the attribute of the data object is the same as the permission value of the permission attribute.

15. (Previously Presented) The system of claim 13 wherein the executable software module causes an indication that a user is permitted to access the attribute sought to be accessed when the value of the attribute of the data object is within a range specified by the permission value of the permission attribute.

16. (Previously Presented) The system of claim 13 wherein the executable software module causes an indication that a user is permitted to access the attribute sought to be accessed when the value of the attribute of the data object is one of enumerated values specified by the permission value of the permission attribute.

17-18. (Canceled)

19. (Previously Presented) The system of claim 13 wherein:
the permission object identifies a permitted action, and
the executable software module causes an indication that a user is permitted to access the attribute sought to be accessed and perform an action on the attribute sought to be accessed when the action is consistent with the permitted action identified in the permission object.

20. (Previously Presented) The medium of claim 1 wherein:
the permission object identifies a permitted action, and
the one or more code segments are further configured to permit the user to access the at least part of data object and perform one or more database operations on the data object when the action is consistent with the permitted action identified in the permission object, where the database operations comprise create, read, update and delete.